Procedure Number	CD 001
Level	3
Issue	1
Issue date	29.11.18
EIA	29.11.18
Review Date	22.11.21
Author	Nick Murton
HoF approval	23.11.18

Edinburgh College

For the future you want

Data Breach Reporting Procedure

Corporate Development

1. BACKGROUND

Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached. The College needs to have in place a robust and systematic process for responding to any reported data security incident, to ensure it can act legally and responsibly, and protect personal data which it processes.

2. AIM

The aim of this procedure is to standardise the College's response to any data breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

- Incidents are reported swiftly and can be properly investigated
- Incidents are dealt with in a timely manner and normal operations restored
- Incidents are recorded and documented
- The impact of the incident is understood, and action is taken to prevent further damage; and incidents are reviewed, and lessons learned
- The ICO and data subjects are informed as required in more serious cases

3. DEFINITION

Article 4 (12) of the General Data Protection Regulation ("GDPR") defines a personal data breach as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

Edinburgh College ('the College') is obliged under the GDPR to act in respect of such data incidents and breaches. This procedure sets out how the College will manage a report of a suspected data security breach. The aim is to ensure that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the incident is properly investigated and reported, and any necessary action is taken to rectify the situation.

There are three types of data breaches. These are:

- Confidentiality breach – unauthorised or accidental disclosure of, or access to, personal data
- Integrity breach – an unauthorised or accidental alteration of personal data
- Availability breach – an unauthorised or accidental loss of access to, or destruction of, personal data

A data security breach can come in many forms, but the most common are as follows:

- Loss or theft of paper or other hard copy
- Data posted, e-mailed or faxed to the incorrect recipient
- Loss or theft of equipment on which data is stored
- Inappropriate sharing or dissemination: staff accessing information to which they are not entitled
- Hacking, malware, and/or data corruption
- Information is obtained by deception or "blagging"
- Equipment failure, fire or flood
- Unescorted visitors accessing data
- Non-secure disposal of data

In any situation where staff are uncertain whether an incident constitutes a breach of security, report it to the Data Protection Officer (DPO) and College Information Manager via **DataProtection@edinburghcollege.ac.uk**

If there are IT issues, such as the security of the network being compromised, IT should also be informed immediately.

Contacts

- Data Protection Officer: **DataProtection@EdinburghCollege.ac.uk**
- College Information Manager: **DataProtection@Edinburghcollege.ac.uk**
- IT Helpdesk: raise a ticket via **TopDesk** on college dashboard/intranet.

4. SCOPE

This college-wide reporting procedure applies to all College information, regardless of format, and must be used by all staff, students, visitors, contractors, partner organisations and data processors acting on behalf of the College. It is to be read in conjunction with the College Data Protection Policy, which is available on the college intranet.

5. RESPONSIBILITES

Information users

All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Incident Response Team

The Information Manager and Data Protection Officer will convene an incident response team who will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable further delegation may be appropriate in some circumstances.

Managers

Heads of Department are responsible for ensuring that staff in their area act in compliance with this procedure and assist with investigations as required.

6. REPORTING A BREACH

Internal

Suspected data security breaches should be reported promptly to the DPO as the primary point of contact: **DataProtection@edinburghcollege.ac.uk.** The report must contain full and accurate details of the incident including who is reporting the incident [and what classification of data is involved]. The incident report form should be completed as part of the reporting process. See Appendix 1.

Once a data incident has been reported an initial assessment will be made to establish whether it is a breach, and the severity of the breach. See Appendix 2. All data security breaches will be centrally logged by the DPO to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

External

Article 33 of the GDPR requires the College as data controller to notify the ICO only when the breach "is likely to result in a risk to the freedoms and rights of natural persons". Such a breach also must be communicated to the data subject (with certain exceptions). Notification must be made "without undue delay" and within 72 hours of becoming aware of it. If the College fails to do this, it must explain the reason for the delay.

Article 33(5) requires that the College must maintain documentation on data breaches, their nature and remedial action taken.

A report to the ICO must contain information as to the nature of the breach, categories of data, number of data records, number of people affected, name and contact details of DPO, likely consequences of the breach and action taken.

7. DATA BREACH MANAGEMENT PLAN

The College's response to any reported data security breach will involve the following four elements.

A. Containment and Recovery
B. Assessments of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Each of these four elements will need to be conducted in accordance with the data breach flowchart, see Appendix 3.
An activity log recording the timeline of the incident management should also be completed. NB. This reflects current guidance from the ICO, which is likely to change.

8. DISCIPLINARY

Staff, students, contractors, visitors or partner organisations who act in breach of college policy and procedure may be subject to disciplinary procedures or other appropriate sanctions.

9. REVIEW

This procedure shall be subject to regular review by the Information Governance Group and shall be revised no later than once every three years.

10. APPENDIX 1: DATA INCIDENT REPORTING TEMPLATE

	Report By:	Name: Click here to enter text. Job Title: Click here to enter text. Department: Click here to enter text. Date: Click here to enter a date.
1.	Summary of event and circumstances	Who, what, when, who etc. Click here to enter text.
2.	Type and amount of personal data	Title of document(s)-what information is included-name, contact details, financial, sensitive or special category data. Click here to enter text.
3.	Action taken by recipient	Click or tap here to enter text.
4.	Action taken to retrieve data and respond to incident	Click or tap here to enter text.
5.	Procedure/policy in place to minimise risk	For example, Edinburgh College Data Protection Policy; IT Facilities Acceptable Use Policy Click here to enter text.
6.	Breach of policy/procedure?	Has there been a breach of policy and has appropriate management action been taken? Click here to enter text.
7.	Complaint received?	Have you received any communication from data subject(s) about this incident Click here to enter text.
8.	Details of Data Protection training provided	Date of most recent training by staff involved Click or tap to enter a date.

11. APPENDIX 2: SEVERITY ASSESSMENT MATRIX

Data Subjects Affected

Description	Scenario	Code Letter	Risk Rating Value
Very High	1000+	VH	5
High	500-999	H	4
Medium	100-499	M	3
Low	10-100	L	2
Very Low	0-10	VL	1

Impact

Description	Score	Code Letter	Risk Rating Value
Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).	VH	5
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).	H	4
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).	M	3
Low	Individuals may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).	L	2
Very Low	No evidence that individuals will be materially affected.	VL	1

Severity

Risk Score = **Data Subjects Affected Score × Impact Score**.

Description	Score	Notify ICO	Notify Data Subjects
Very High	20+	Yes	Yes
High	16-19	Yes	Consider
Medium	11-15	Consider	Consider
Low	6-10	No	No
Very Low	1-5	No	No

A final decision about notification to ICO, and whether to inform the data subjects will be made by the Information Management Team, in conjunction with the college's Data Protection Officer.

12. APPENDIX 3: DATA BREACH PROCEDURE FLOWCHART